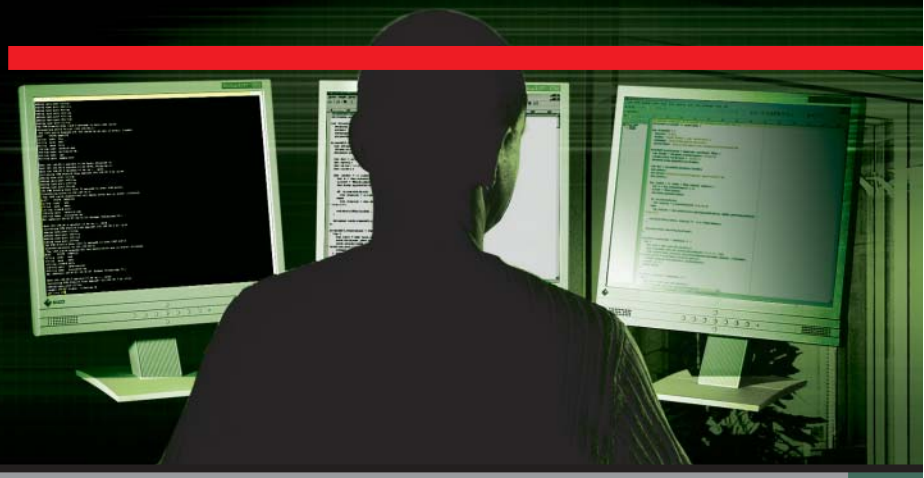


CSI: Internet

5. část

E-mailová zlodějna

Phishingová mafie je čím dál tím rafinovanější. Tým CSI odhalil cílený útok v internetové kavárně – a vykázal hackera do patřičných mezí. *Valentin Pletzer, autor@chip.cz*

Půjde-li to tak dál, můžu své internetové kavárny rovnou zavřít," naříká pan D. „Už jsem přišel o první zákazníky." A ukazuje nám výtisky mailů, které byly během posledních dvou týdnů odeslány jen návštěvníkům jeho řetězce internetových kaváren. Jsou tím zneklidněni jak zákazníci, tak pochopitelně i podnikatel.

Tyto phishingové maily jsou téměř bezchybně formulovány, a příjemce dokonce oslovují jeho správným jménem. Na první pohled jsou tak od legitimních e-mailů k nerozeznání. A jejich obsah? „V průběhu technické údržby nyní kontrolujeme všechny uživatelské účty. Navštivte prosím obratem následující webovou stránku. Pokud tuto výzvu neuposlechnete, budeme nuceni váš účet zrušit a vaše pohledávka propadne."

Neobvyklý phishingový mail však není jediným problémem. Někteří zákazníci se také domnívají, že čísla jejich kreditních karet se na internet dostala právě v internetových kavárnách. To se sice nedá dokázat, nicméně poškozená image znamená pro řetězec kaváren těžkou úhonu. Poněvadž udávaná webová stránka (cíl phishingu) je on-line pokaždé jen velmi krátkou dobu, pan D. o ní mnoho neví. Jedno je však jasné: zadání hesel nebo zákaznických údajů, jak je na phishingových stránkách jinak obvyklé, se zde nepožaduje. Náš tým proto musí nejprve vypátrat, co pachatel vlastně zamýšlí.

Pro začátek se tedy důkladněji rozhlížíme po internetové kavárně. Funguje tak, jako všechna podobná zařízení: návštěvník zde za poplatek smí surfovat na internetu, buď prostřednictvím místní „surfovací stanice", nebo s vlastním notebookem přes bezdrátovou síť. Platí se u pokladny nebo kreditní kartou. Každý zákazník obdrží své zcela individuální konto, takže z něj může hradit poplatky v každé kavárně celého řetězce.

Místo činu: Internetová kavárna

OBĚTI: Mnozí návštěvníci internetových kaváren nemají vlastní počítač a v této problematice se vyznají jen povrchně – to je pro každého hackera samozřejmě perfektní cílová skupina.

Z obětí útočníci

Náš vyšetřovatelský tým zahajuje pátrání u jediného záchytného bodu – phishingového mailu. Mnoho nadějí v něj však nevkládáme: takové maily, podobně jako spam, bývají obvykle rozesílány sítí botů. To téměř znemožňuje nalezení původců. Odesílatelé jsou v těchto případech sami jen hackerovou obětí. Žádáme pana D., aby nám e-maily poskytl v elektronické formě. Na výtisku totiž není vidět hlavička zprávy, tzv. „E-mail header". Při troše štěstí by nám mohla prozradit, ze kterého serveru byla zpráva odeslána.

Marná snaha! Jak jsme se obávali, maily nebyly rozesílány z regulérního serveru. Přece jen však rychle zjišťujeme, že udaný e-mailový server má IP adresu jednoho z polských poskytovatelů DSL. Pravděpodobně se tedy některý ze zákazníků tohoto poskytovatele rovněž stal obětí útočníka. Po dotazu u poskytovatele se však dozvídáme jen to, že inkriminovaná IP adresa skutečně patří jednomu z jeho zákazníků. Další pomoc nám

Nový seriál Chipu

V americkém kriminálním seriálu o CSI objasňují vyšetřovatelé zločiny pomocí vědeckých metod. Chip si vzal „Kriminálku Las Vegas" za vzor pro novou řadu článků, která ukáže, jak profesionální vyšetřovatelé a specialisté bojují proti strmě narůstající počítačové kriminalitě.

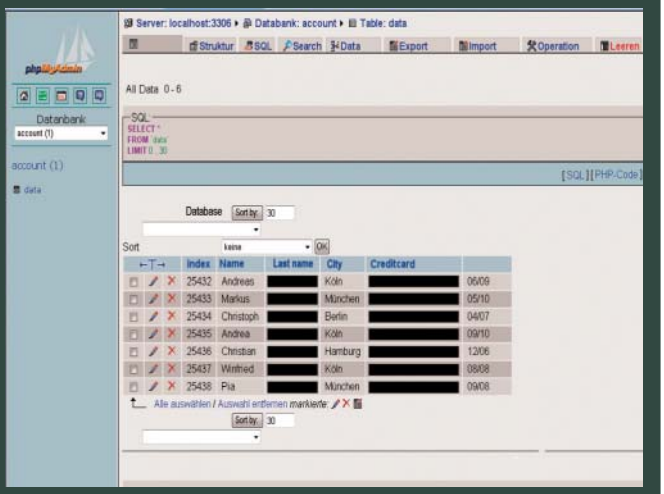
byla odepřena. „Ochrana osobních údajů," říká provider. Dočkáme se však alespoň příslibu, že dotyčný zákazník bude o útoku informován.

Ani naše druhá stopa, odkaz na webovou stránku v e-mailu, nás nedovede dále. Adresa je už dlouho nedostupná. To nás příliš nepřekvapuje, neboť takové stránky bývají zpravidla aktivní jen velmi krátkou dobu. I kdyby totiž byla stránka zablokována, přijde další útok odjinud – a většinou se server přemístí do jiné země. Trestní stíhání je tak prakticky nemožné.

Past na hackera

Nezbývá než nasadit účinnější prostředky – rozhodujeme se nastražit hackerovi léčku. V internetové kavárně se hlásíme jako zákazníci, a to s jedním kontem na surfovací stanici a jedním na WLAN a notebook. Co se děje pak, překvapí i nás. Už za několik minut dostáváme první phishingový mail – příliš rychle, než aby šlo o pouhou náhodu. Po krátkém zkoumání objevujeme příčinu: chatovací prostor kavárny. Kdo je totiž on-line, je automaticky přihlášen i tam. Problém spočívá v tom, že jméno uživatele je součástí mailové adresy – ta je sestavena podle schématu „jméno.příjmení@doména.de". Pro hackera je potom snadné nejen zjistit adresy, ale i jmenovitě oslovit adresáty.

Kořist



ZLATÝ DŮL
Kompletní datové věty zákazníků z pečlivě udržovaných databank jsou žádaným cílem hackerů.

Pak už jde všechno ráz na ráz. Máme teď dvě další stopy. Jednak odkaz udaný v mailu, který je natolik čerstvý, že ještě vede na dosud existující stránku. A kromě toho je také jasné, že hacker musí být stálým účastníkem chatu – a jeho IP adresu tedy najdeme v log souboru serveru.

Hackerova webová stránka je opravdu ještě on-line – a odhaluje nám tajemství jeho motivu: hacker má spadeno na ústřední databanku internetové kavárny. Z ní si vytáhne zákaznická data, jako čísla kreditních karet a e-mailové adresy. A při tom mu pomáhají jeho oběti: jelikož je síť internetové kavárny „obehnána" firewallem, potřebuje hacker někoho, kdo mu zevnitř otevře vstupní vrátka – kliknutím na odkaz v e-mailové zprávě. Jakmile totiž někdo za firewallem otevře webovou stránku, aktivuje se zvláštní javascript. Tak si hacker pomocí kombinace „Cross-Site-Scripting" a „SQL-Injection" stáhne z databankového serveru internetové kavárny citlivé informace o jejích zákaznících. V odborném žargonu se tomu říká „Drive-by-Hacking".

EXPERT

Zulfikar Ramzan je bezpečnostním specialistou firmy Symantec. Varuje před „Drive-by-Hackingem", k jehož úspěšnosti stačí návštěva jedné zmanipulované webové stránky.

Uzavřít vstupní brány

Ke konzultaci jsme také povolali bezpečnostního experta. „Nejen firmy se musí mít před tímto druhem útoků na pozoru," říká Zulfikar Ramzan z firmy Symantec. „Oběťmi Drive-by-Hackingu se mohou stát především směrovače ve WLAN a DSL." Trik je pokaždé stejný jako v našem případě: hacker rozešle odkaz na připravenou webovou stránku. Jakmile ji oběť otevře, spustí se javascript v prohlížeči – a tedy za firewallem. Pak už není těžké směrovač zmanipulovat a otevřít bránu do sítě.

Teď bychom samozřejmě chtěli pohnat hackera k odpovědnosti. Ten je však stále o krok před námi. Sice v protokolu chatovacího serveru jako naši druhou stopu zanechal svou IP adresu, ta však vede jen na server anonymizační služby. Tady naše stopa končí. Přesto jsme jistý drobný úspěch zaznamenali: pan D. bude napříště své servery – a tím i zákazníky – lépe chránit. Hackerova vstupní brána bude uzavřena a jména uživatelů už nebudou dostupná. To však za žádnou definitivní ochranu považovat nelze. Hackeři vynalézají stále nové triky – a už v příštím pokračování našeho seriálu „CSI: Internet" vám odhalíme další z nich.

Valentin Pletzer

VÍCE INFORMACÍ

www.symantec.com: Bezpečnostní firma zabývající se nejen narůstajícím nebezpečím „Drive-by-Hackingu".